AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-22 (canceled)

23. (Previously Presented) A method of securely authenticating subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

performing a first run of an authentication and key agreement procedure in the radio communication network, between a mobile node and an authentication server of the radio communication network, so as to authenticate the mobile node to the radio communication network;

initiating an authentication procedure with a stable forwarding agent of the mobile routing system;

performing a second run of the authentication and key agreement procedure between the mobile node and the authentication server so as to generate a shared secret;

providing the shared secret to the stable forwarding agent and using the shared secret to authenticate the mobile node to the stable forwarding agent;

sending a public key from the mobile node to the stable forwarding agent;

agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured;

following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from said authentication server;

using the subscriber contact information to assign a Fully Qualified Domain Name and/or IP address to the mobile node; and

updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address and the public key provided by the mobile node.

24. (Previously Presented) A method according to claim 23, further comprising:

transporting messages associated with the second run, between the stable forwarding agent used by a mobile node and the authentication server via the stable forwarding agent.

25. (Previously Presented) A method according to claim 23, further comprising:

sending session keys, agreed upon during the second run of the authentication procedure, from the authentication server to the stable forwarding agent.

26. (Previously Presented) A method according to claim 23, further wherein the mobile routing system is a Mobile IP based system, and the stable forwarding agent is a Home Agent.

27. (Previously Presented) A method according to claim 23, wherein the mobile routing system is a HIP based system.

28. (Previously Presented) A method according to claim 23, wherein said authentication and key agreement procedure is the Authentication and Key Agreement procedure specified by 3GPP.

29. (Previously Presented) A method according to claim 23, wherein the collected subscriber contact information comprises one or more of the following:

the name and postal address of a subscriber;

the telephone number associated with a subscriber;

the existing Fully Qualified Domain Name for a subscriber; and

the status of any mobility services established earlier for a subscriber.

30. (Currently Amended) A stable forwarding agent of a mobile routing system for use in securely authenticating subscriber and security data in ~~a~~ the mobile routing system, the mobile routing system having ~~when the~~ subscribers who are also subscribers of a radio communication network, where a first run of an authentication and key agreement procedure has been performed in the radio communication network between a mobile node and an authentication server of the radio communication network so as to authenticate the mobile node to the radio communication network, the stable forwarding agent comprising:

a relay for relaying messages associated with a second run of the authentication and key agreement procedure between the mobile node and the authentication node of the radio communication network, the second run resulting in generation of a shared secret;

a receiver for receiving and using the shared secret to authenticate the mobile node, for collecting subscriber contact information from the authentication server, and for receiving a public key from the mobile node;

a key determining processor for agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured; and

a mobility service provisioning processor for using the subscriber contact information to assign a suitable Fully Qualified Domain Name and/or IP address to said mobile node and for updating a subscriber database and DNS server with the Fully Qualified Domain name and/or IP address and the public key provided by the mobile node.